Claims

1. Method for generating a second data stream from a first data stream which comprises a first header (12) and a first payload data block (14) with payload data, the method comprising the following steps:

extracting (116) the first header (12) from the first data stream;

generating (118) a second header for the second data stream;

entering (120) at least a part (42, 44, 74) of the first header into the second header, the part of the first header including information which allows conclusions as to the origin of the payload data; and

generating (122) a second payload data block having the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

2. Method as claimed in claim 1, wherein the information allowing conclusions as to the origin of the first data stream includes an identification (42) for a supplier of the first data stream.

3. Method as claimed in claim 1 or 2, wherein the information allowing conclusions as to the origin of the first data stream includes author information (74), such as the author, the component, the ISRC number, the ISAN number or the ISMN number of the payload data of the first data stream.

4. Method as claimed in any of the preceding claims, wherein the part of the first header, which is entered

into the second header, further comprises an identification (44) of the receiver of the first data stream.

5. Method as claimed in claim 4, wherein the identification is device-specific, and the receiver (104) of the first data stream is a player indicated by the identification, or a smart card.

6. Method as claimed in any of the preceding claims, wherein the part of the first header which is entered into the second header further comprises licence data (30) relating to the manner in which a receiver (104) of the first data stream may use the same, the licence data of the first header specifying the licence data of the second header.

7. Method as claimed in claim 6, wherein the licence data (30) of the first header specify that the first data stream may be copied a certain number of times (62), that no copy my be taken of a copy, however, the step of generating (118) the second header for the second data stream including the entering of second licence information into the second header of the second data stream, such that no more copy may be taken of the second data stream.

8. Method as claimed in any of claims 4 to 7,

wherein the step of generating (118) a second header comprises the step of entering an identification (44) for the receiver (106a to 106c) of the second data stream as a user identification, and of entering an identification of the receiver (104) of the first data stream as a supplier identification (42), and

wherein the step of entering (120) at least a part of the first header into the second header comprises the entering of the identification of the supplier (42)

of the first data stream as a supplier identification, and the entering of the identification (44) of the receiver of the first data stream as a user identification into a part of the second header, which is reserved for information of the first header.

9. Method as claimed in any of the preceding claims which further comprises the following step:

issuing a digital signature (66) for the second header, including the part of the first header, and attaching the digital signature to the second header.

10. Method as claimed in claim 9, wherein the issuing step further comprises the following substeps:

forming a hash sum over the second header, including the part (34) of the first header, using a specified hash algorithm (68); and

encrypting the hash sum by means of an asymmetric encrypting method using a private key of the receiver (104) of the first data stream.

11. Method as claimed in any of the preceding claims, wherein the payload data in the payload data block (14) are at least partly encrypted and wherein encrypting information is contained in the first header, the step of generating (118) the second header further comprising the following steps:

decrypting the first payload data block of the first data stream using the encrypting information (46, 40, 22 to 26) in the first header;

encrypting the decrypted payload data and entering corresponding encrypting information (46, 40, 22 to 26) into the second header,

the encrypting information of the first header also being entered into the second header.

12. Method as claimed in claim 11, wherein the encrypted payload data in the first payload data block (14) are encrypted symmetrically and wherein the key is again encrypted asymmetrically using a private key, the decrypting step comprising the following steps:

decrypting the encrypted key (46) by means of the public key of the supplier (102) so as to obtain the key for a symmetric decryption (40);

encrypting a payload data key of the decrypted payload data using a private key of a receiver (104) of the first data stream carrying out the method for generating a second data stream; and

entering the asymmetrically encrypted payload data key into the second header (46).

13. Method as claimed in any of the preceding claims, wherein in the step of entering (120), the entire first header is entered into the second header.

14. Method as claimed in any of the preceding claims, wherein the first header itself comprises at least a part of a header of a data stream which relates to the origin of the first data stream, such that the entering step results in a multiply recursive header structure (Fig. 5).

15. Method for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, wherein at least a part (70) of the first

header which comprises information regarding the origin of the first data stream, is contained in the second header, the method comprising the following steps:

extracting (132) the part (70) of the first header from the second header;

verifying (134) the origin of the second data stream using the part (70) of the first header which comprises information regarding the origin of the first data stream; and

in case of a positive result of the verifying step (136), playing (140) the second data stream.

16. Method as claimed in claim 15, wherein the second header of the second data stream has a digital signature (66) attached to it which fits the part (70) of the first header, and wherein the verifying step comprises the following substep:

checking the authenticity of the second header using the digital signature (66).

17. Method as claimed in claim 16, wherein the digital signature (66) is the result of an encryption of a hash sum of the second header, which encryption has been carried out by means of a private key of the apparatus (104) having generated the second data stream, the step of checking the authenticity comprising the following steps:

decrypting the digital signature by a public key of the apparatus (104) which has generated the second data stream, so as to obtain the hash sum of the second header;

forming a hash sum of the present header;

comparing the hash sums;

in case of the hash sums matching, issuing a positive verification result (136).

18. Method as claimed in claim 17, wherein the part (70) of the first header further comprises licence information (30) regarding the manner in which the first data stream may be utilized, and wherein the second header comprises licence data (30) derived from the licence data of the first header, the method further comprising the following substeps:

comparing the licence data of the second header and the first header so as to evaluate the authenticity of the licence data of the second header;

in case of questionable authenticity, blocking (138) the playing of the second data stream.

19. Apparatus (104) for generating a second data stream from a first data stream which comprises a first header (12) and a first payload data block (14) with payload data, the apparatus comprising the following:

means for extracting (116) the first header (12) from the first data stream;

means for generating (118) a second header for the second data stream;

means for entering (120) at least a part (42, 44, 74) of the first header into the second header, the part of the first header including information which allow conclusions as to the origin of the payload data; and

means for generating (122) a second payload data block which comprises the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

20. Apparatus (104) as claimed in claim 19, which is designed as a personal computer.

21. Apparatus (106a to 106c) for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, at least a part (70) of the first header, which comprises information regarding the origin of the first data stream, being contained in the second header, the apparatus comprising the following:

means for extracting (132) the part (70) of the first header from the second header;

means for verifying (134) the origin of the second data stream using the part (70) of the first header which comprises information regarding the origin of the first data stream; and

means for playing the second data stream, which responds to the means for verifying (134), so as to play the second data stream only if the means for verifying (134) provide a positive result.

22. Apparatus as claimed in claim 21, which is designed as a hifi system (106b), as a car hifi system (106a), as a portable multimedia player (106c), as a computer or as a component of any of the above-mentioned devices.